



Functional Safety Engineering

Practical SIL Determination Methods

based on

IEC 61511

ProSalus Limited

Slide 7 - 1



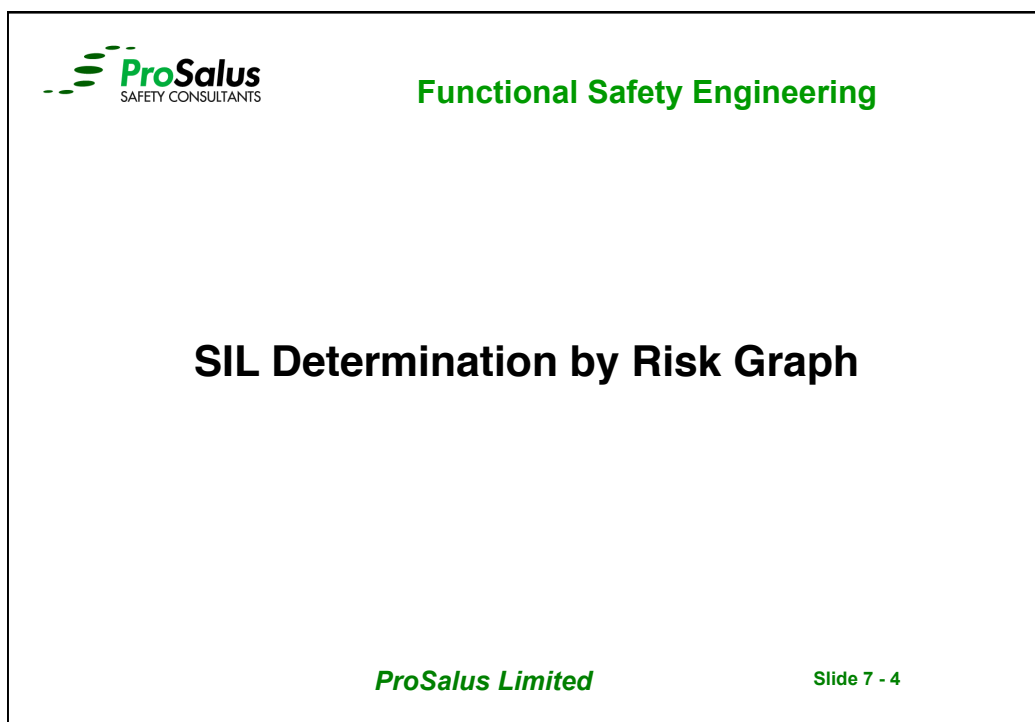
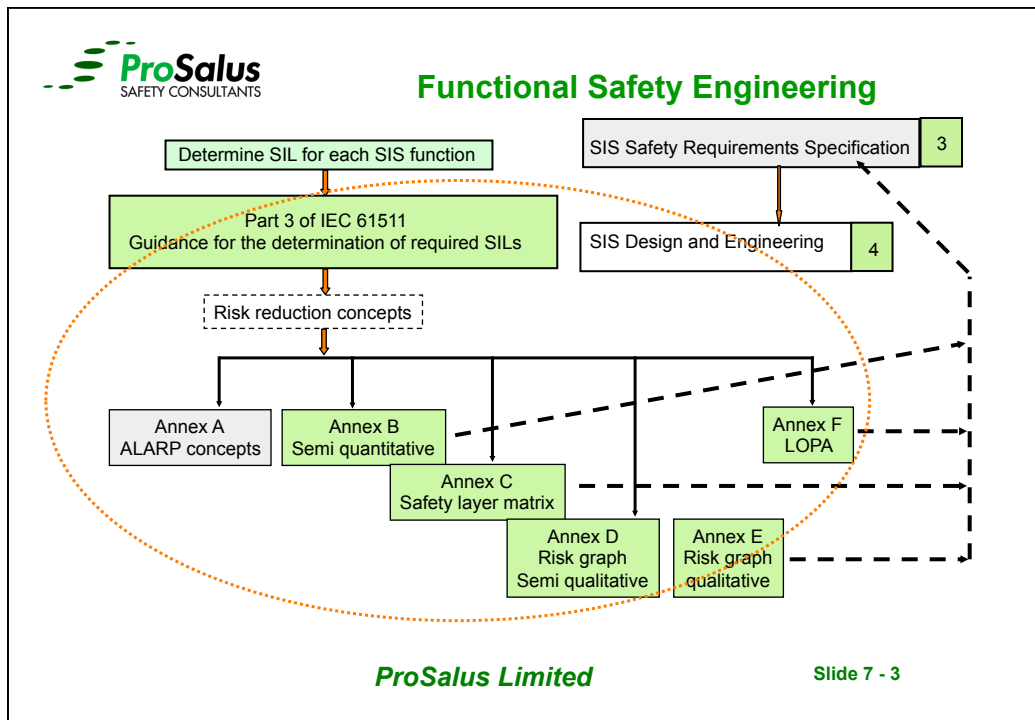
Functional Safety Engineering

Target Safety Integrity Level (SIL) of a SIF

- The target SIL of the SIF is critical to the SRS
 - To ensure the design is appropriate to the risk contribution required to prevent the hazard from occurring
- IEC 61511-3 provides guidance on determination methodologies
- CCPS also offers guidance on the LOPA method
- These methods can be quantitative, semi quantitative or qualitative methods

ProSalus Limited

Slide 7 - 2





Functional Safety Engineering

The Risk Graph Assessment Team

- Competent, Experienced team with relevant site experience and knowledge of the process to be assessed
- Based on the Process to be assessed the team should include:
 - Independent Facilitator & Scribe (Could be Process Safety Engineer)
 - Process design experience
 - Operations experience
 - Maintenance experience & equipment knowledge
 - Safety representative
 - Control & Instrument representative
 - Other specialists as required (Electrical, Mechanical, Equipment vendor)

ProSalus Limited

Slide 7 - 5




Functional Safety Engineering

Risk Graph

- Determination Tool Based on Calibrated Risk Parameters (IEC 61511-3):
 - Demand Rate (W)
 - Consequence (C)
 - Occupancy (F)
 - Probability of Avoidance (P)
- Mandatory to consider Personal Safety and Environment consequences
- Optional to consider Asset consequences / business needs
- Now considered a screening tool for significant risk SIFs
- Tend to be conservative
- Can be Qualitative or Semi Quantitative

ProSalus Limited

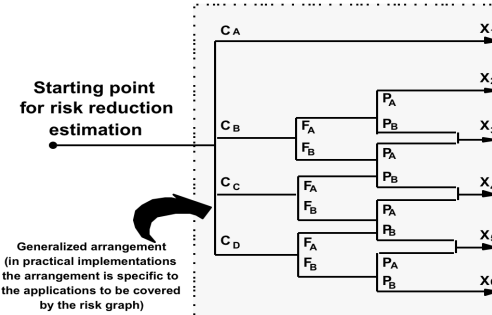
Slide 7 - 6



Functional Safety Engineering

Risk graph: general scheme

Starting point for risk reduction estimation




Generalized arrangement
(in practical implementations the arrangement is specific to the applications to be covered by the risk graph)

w_3	w_2	w_1
a	---	---
1	a	---
2	1	a
3	2	1
4	3	2
b	4	3

--- = No safety requirements
 a = No special safety requirements
 b = A single E/E/PES is not sufficient
 1, 2, 3, 4 = Safety integrity level

ProSalus Limited

Slide 7 - 7



Functional Safety Engineering

Personal Safety Risk Graph

- Based on the IEC61511-3 Methodology (Also guidance in IEC 61508-5, Annex D)
- Calibrated in terms of potential loss of life
- All four risk parameters (W, C, F, P) considered:
 - The Frequency of Demand with no SIS installed
 - Consequences in terms of fatalities or serious injury with no SIS installed
 - Personal exposure to the hazard in terms of occupancy
 - Duration is normally assessed as less than 10% or more than 10% of working time
 - Probability of Avoidance
 - Avoidance factors such as SIS failure alarm, manual shutdown & evacuation

ProSalus Limited

Slide 7 - 8

Risk graph: Semi Quantitative Parameters

Parameter	Range of values
<p><u>Consequence: C</u></p> <p>Number of Fatalities Guidance as follows:</p> <p>Multiply no of people present when area is occupied by vulnerability.</p> <p>Vulnerability factors guide:</p> <p>V = 0.01 small release of flammable or toxic material</p> <p>V = 0.1 Large release</p> <p>V = 0.5 As above but high probability of fire or highly toxic</p> <p>V = 1 Rupture or explosion.</p>	<p>C_A = Minor injury</p> <p>C_B = Range 0.01 to < 0.1</p> <p>C_C = Range 0.1 to < 1.0</p> <p>C_D = Range > 1.0</p>

ProSalus Limited

Slide 7 - 9

Risk graph: Semi Quantitative Parameters

Parameter	Range of Values
<p>Occupancy (F)</p> <p>This is calculated by determining the length of time the area exposed to the hazard is occupied during a normal working period</p> <p>Avoidance (P)</p> <p>Possibility of avoiding the hazardous event if the protection system fails to operate.</p>	<p>F_A = Rare to more often exposure in the hazardous zone. Occupancy less than 0.1</p> <p>F_B = Frequent to permanent exposure in the hazardous zone.</p> <p>P_A = Possible to avoid</p> <p>Should only be selected if all the following are true:</p> <p>Facilities are provided to alert the operator that the SIS has failed</p> <p>Independent facilities are provided to shut down such that the hazard can be avoided or which enable all persons to escape to safe area</p> <p>The time between the operator being alerted and a hazardous event occurring exceeds 1 hour</p> <p>P_B = Not possible to avoid. Applies if any of P_A conditions are not met</p>

ProSalus Limited

Slide 7 - 10

Risk graph: Semi Quantitative Parameters

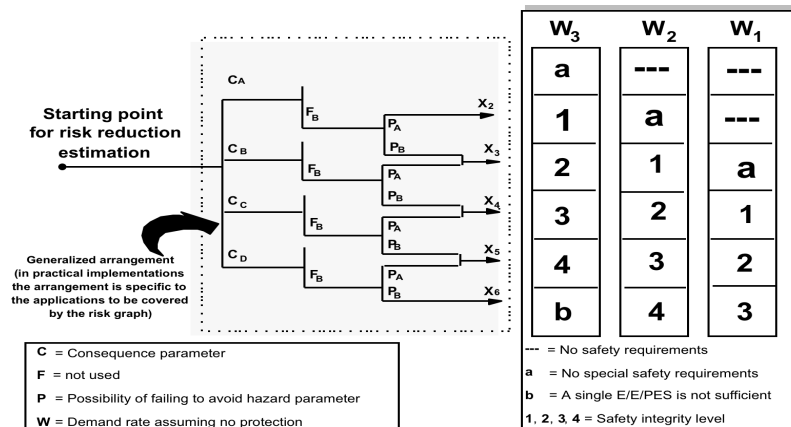
Parameter	Range of Values
Demand rate (W). The number of times per year that the hazardous event would occur in the absence of the SIS under consideration	W_1 = Demand rate less than 0.1 demand per year
	W_2 = Demand rate between 0.1 demand and 1 demand per year
	W_3 = Demand rates higher than 1 demand and 10 demands per year

Demand Rates (W)

Demand rates are generally determined by:

- Control system failure
- Equipment Failure such as pumps, valves, blockage etc
- Human error;
- During abnormal operating conditions e.g. start up;
- Environmental conditions;
- Utility failure e.g. electrical, instrument air, cooling water etc.

Risk Graph: Environmental Impact



ProSalus Limited

Slide 7 - 13

General environmental consequences

Risk parameter	Classification	Comments
Consequence (C) C_A	A release with minor damage that is not very severe but is large enough to be reported to plant management	A moderate leak from a flange or valve Small scale liquid spill Small scale soil pollution without affecting ground water
C_B	Release within the fence with significant damage	A cloud of obnoxious vapour travelling beyond the unit following flange gasket blow-out or compressor seal failure
C_C	Release outside the fence with major damage which can be cleaned up quickly without significant lasting consequences	A vapour or aerosol release with or without liquid fallout that causes temporary damage to plants or fauna
C_D	Release outside the fence with major damage which cannot be cleaned up quickly or with lasting consequences	Liquid spill into a river or sea A vapour or aerosol release with or without liquid fallout that causes lasting damage to plants or fauna Solids fallout (dust, catalyst, soot, ash) Liquid release that could affect groundwater

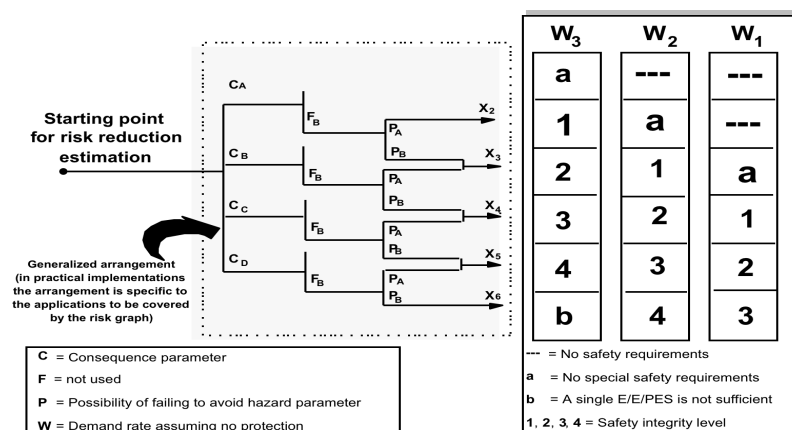
ProSalus Limited

Slide 7 - 14

Asset Loss graph

- The severity of the consequence are calibrated:
 - In terms of Financial loss
 - The financial consequences must be calibrated in terms of what would occur if no SIS installed
 - Beware of over extending the financial loss as the leads to high SIL values were the SIS would have had no impact

Risk Graph: Asset Loss



General asset consequences (Not in IEC 61511)

Risk Parameter		Classification for Asset in £	
Consequence (C)	C _A	Impact of 100,000 – 1,000,000	
	C _B	Impact of 1,000,000 – 10,000,000	
	C _C	Impact of 10,000,000 – 100,000,000	
	C _D	Impact of > 100,000,000	

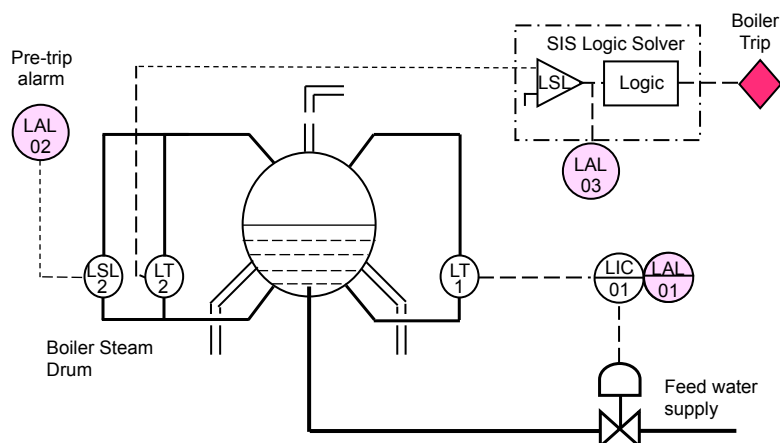
A credit is an Order of Magnitude (SIL1)


- Don't take credit for the control system when it was the cause of the demand
- Don't take credit for the SIS which the SIF under assessment forms a part of
- Don't take a credit for frequency of occupancy when there is uncertainty in the location of operations / maintenance
- Don't take a credit for avoidance unless all of the criteria can be met
- A SIF can protect against more than one hazard, assess each hazard in turn and take the worse case SIL

The Target Integrity Level

- The target integrity of a SIF is determined from the highest of the three assessment:
 - Safety
 - Environment
 - Asset
- Target Integrity level = maximum (SIL, EIL, AIL)
- The SIF must be designed to achieve the highest target Integrity Level

Boiler Drum with pre-trip alarm and SIS trip Example





Functional Safety Engineering

Risk Parameters: SIL Classification by Risk Parameters Chart

C – Extent of Damage

C_A : Slight injury
 C_B : Severe irreversible injury to one or more persons or death of a person
 C_C : Death of several persons
 C_D : Catastrophic consequences multiple deaths

F – Frequency & Exposure time

F_A : Seldom to relatively frequent
 F_B : Frequent to continuous

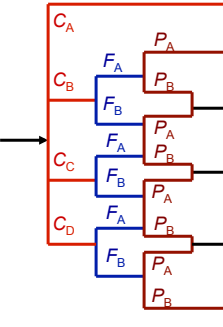
P – Hazard Avoidance / Mitigation

P_A : Possible under certain conditions
 P_B : Hardly possible

W – Occurrence Probability

W_1 : Very low
 W_2 : Low
 W_3 : Relatively high

Starting point




	W_3	W_2	W_1
C_A	a	-	-
C_B	1	a	-
C_C	2	1	a
C_D	3	2	1
C_D	4	3	2
C_D	b	4	3

- = No safety requirements
a = No special safety requirements
b = A single E/E/PES is not sufficient
1,2,3,4 = Safety integrity level

ProSalus Limited

Slide 7 - 21



Functional Safety Engineering

SIL Classification by Risk Parameters Chart: Example

C – Extent of Damage

C_A : Slight injury
 C_B : Severe irreversible injury to one or more persons or death of a person
 C_C : Death of several persons
 C_D : Catastrophic consequences multiple deaths

F – Frequency & Exposure time

F_A : Seldom to relatively frequent
 F_B : Frequent to continuous

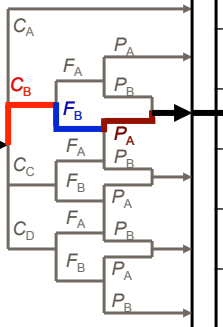
P – Hazard Avoidance / Mitigation

P_A : Possible under certain conditions
 P_B : Hardly possible

W – Occurrence Probability

W_1 : Very low
 W_2 : Low
 W_3 : Relatively high

Starting point



	W_3	W_2	W_1
C_A	a	-	-
C_B	1	a	-
C_B	2	1	a
C_C	3	2	1
C_D	4	3	2
C_D	b	4	3

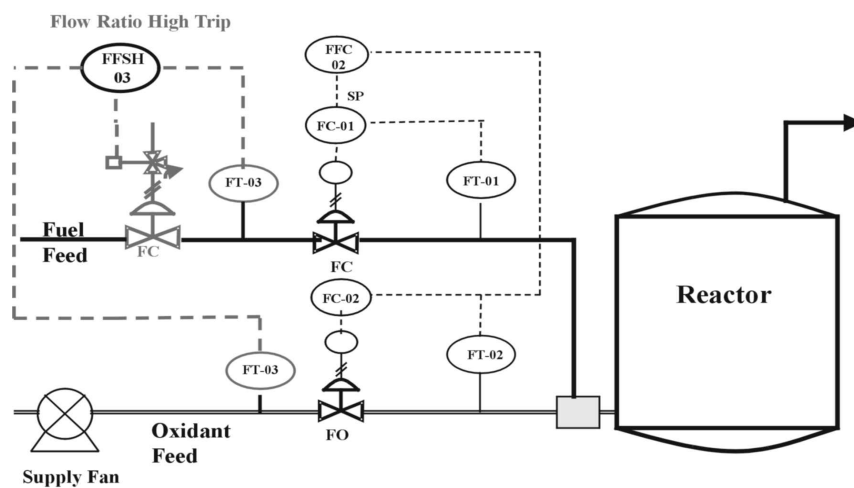
- = No safety requirements
a = No special safety requirements
b = A single E/E/PES is not sufficient
1,2,3,4 = Safety integrity level

ProSalus Limited

Slide 7 - 22

Practical Exercise No: 3

Determination of SIL by Risk Graph





Functional Safety Engineering

Exercise No: 3 - Determination of SIL by Risk Graph

This practical exercise requires participants to determine the required SIL of a proposed safety-instrumented system using the basic principles and risk graphs and calibration parameters for safety, environment and asset loss described in this module

The process is a reactor with a continuous feed of fuel and oxidant. Two flow control loops are operated under a ratio controller set by the operator to provide matching flows of fuel and oxidant to the reactor. An explosive mixture can occur within the reactor if the fuel flow becomes too high relative to the oxidant flow.

Possible causes are: Failures of the BPCS or an Operator error in manipulating the controls Sudden loss of oxidant feed.

A SIS is proposed with a separate set of flow meters connected to a flow ratio measuring function that is designed to trip the process to safe condition if the fuel flow exceeds the oxidant flow by a significant amount

The tag number for this function is FFSH- 03

ProSalus Limited

Slide 7 - 25



Functional Safety Engineering

Assume that the following information has been decided for the reactor.

The total frequency of the events leading to an explosive mixture is approximately once every ten years.

The consequence of the explosion has been determined to be a vessel rupture causing death or serious injury to 1 person

The occupancy in the exposed area is less than 10% of the time and is not related to the condition of the process.

The onset of the event is likely to be fast with a worst-case time of 10 minutes between loss of oxidant and the possible explosion.

The material released from an explosion is not harmful to the environment.

The reactor will cost in excess of £250, 000 to replace.

Determine the target SIL = , EIL = , AIL =

Determine the overall target integrity for the SIF =

ProSalus Limited

Slide 7 - 26



Functional Safety Engineering

ProSalus Limited

Slide 7 - 27

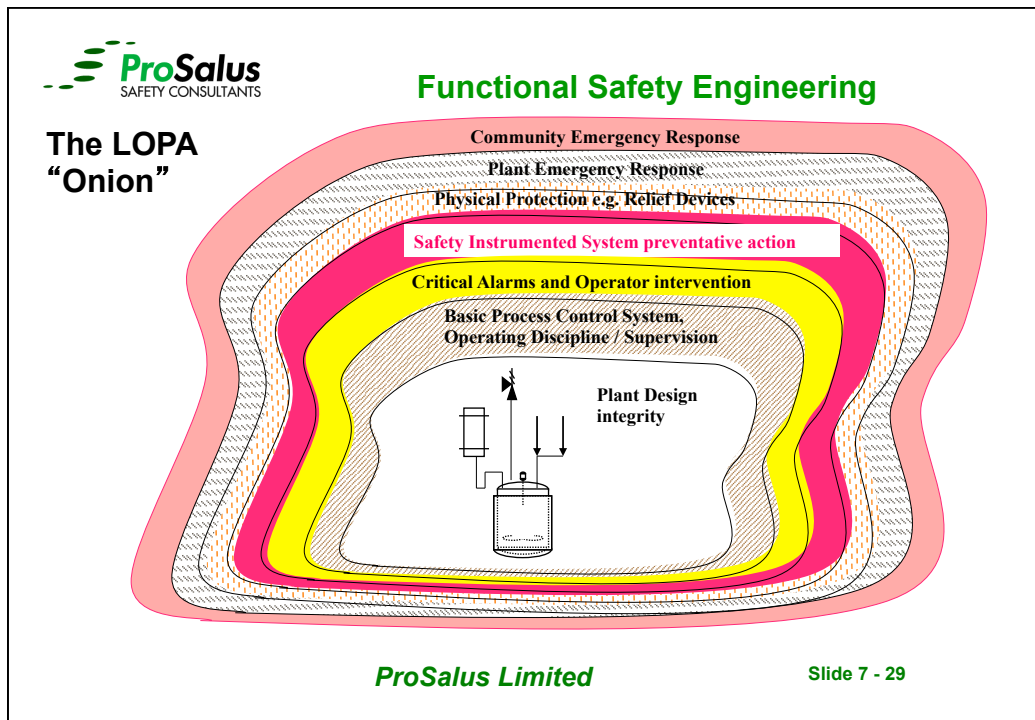


Functional Safety Engineering

Layers of Protection Analysis (LOPA)

ProSalus Limited

Slide 7 - 28



ProSalus
SAFETY CONSULTANTS

Functional Safety Engineering

- **What is LOPA**
 - Usually developed from HAZOP introduced in 2001 per IEC 61511
 - Assessment usually hazard scenario based (i.e derived from HAZOP)
 - It is a modified version of ETA usually based on the CCPS simplified process risk assessment approach and is considered a semi quantitative type analysis.
 - For "Buncefield Type" scenarios (Storage Tanks) a more Quantitative approach is required
 - For IEC 61511 analyses each hazard cause / consequence pair where a SIF has been identified as a safe guard during HAZOP
 - Can be applied to general PRA without SIF assessment
 - Requires Tolerability Risk Criteria to be established for site under assessment

ProSalus Limited Slide 7 - 30

IEC 61511 - Mapping HAZOP Data to LOPA Data

LOPA REQUIRED	HAZOP DEVELOPED
INFORMATION	INFORMATION
Impact Event	Consequence
Severity Level	Consequence Severity
Initiating Cause	Cause
Initiating Likelihood	Cause Frequency
Protection Layers	Existing Safeguards
Required Additional Mitigation	Recommended New Safeguards

The LOPA Process:

1. Define the unwanted Impact
2. Determine and list all of the initiating events
3. Determine and list all of the layers of protection
4. Quantify the frequency of the initiating events
5. Quantify the effectiveness of the layers of protection
6. Calculate the resultant frequency of the unwanted impact



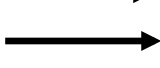
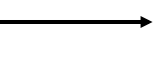

Functional Safety Engineering LOPA Worksheet

	1	Impact Event		
Likelihood are event/year and protection are PFD Average	2	Severity Level		
	3	Initiating Cause		
	4	Initiation Likelihood		
Protection & Mitigation Layers	5	General Design		
		Control System		
		Independent Alarm		
	6	Additional Mitigation, restricted access		
	7	Additional Mitigation		
	8	Intermediate Event Likelihood		
	9	PFDavg required		
	10	Tolerable Mitigated Event Likelihood		
	11	Notes		

ProSalus Limited

Slide 7 - 33

Functional Safety Engineering How LOPA works

		Example
	Risk Tolerance Criteria (freq.)	10^{-7}
	Initiating Event Frequency	10^{-1}
	Conditional Modifier (Ignition Frequency)	10^{-1}
	PFD of 1st IPL (BPCS)	10^{-1}
	PFD of 2nd IPL (Mechanical PRV)	10^{-2}
	SIL (1-3) for SIS₁	$10^{-?}$
	SIS Required. $SIL = 10^{-7}/(10^{-1}*10^{-1}*10^{-1}*10^{-2}) = 10^{-2}$	

ProSalus Limited

Slide 7 - 34



Functional Safety Engineering

IEC 61511 Part 3 Annex F.4 Severity Levels

Table F.2 Impact event severity levels

Severity Level	Consequence
Minor (M)	Impact initially limited to local area of event with potential for broader consequence, if corrective action not taken
Serious (S)	Impact event could cause serious injury or fatality on site or offsite
Extensive (E)	Impact event that is five or more severe times than a serious event

ProSalus Limited

Slide 7 - 35



Functional Safety Engineering

Example Personnel Risk Tolerance Criteria

Defined Severity Level	Safety Consequence Descriptors	Maximum Frequency of Mitigated Event Likelihood/yr
Minor (Ms)	Serious injury to employee (probability of death <10%)	1×10^{-4}
Serious (Ss)	Potential loss of life of one or more employees (probability of death > 10%). Serious injury to member of public (probability of death <10%)	1×10^{-5}
Extensive (Es)	Potential loss of life of many employees (greater than 3 and up to 10) Potential loss of life of one or more members of the public (probability of death >10%)	1×10^{-6}
Catastrophic (Cs)	Potential loss of life of many people (10 – 100)	Use QRA

ProSalus Limited

Slide 7 - 36

Example Environmental Risk Tolerance Criteria

Defined Severity Level	Safety Consequence Descriptors	Maximum Frequency of Mitigated Event Likelihood/yr
Minor (Ms)	NOTICEABLE – On site reportable – A release with minor damage that is not very severe, but is large enough to be reported to plant management	3×10^{-3}
Serious (Ss)	SIGNIFICANT – On site short term – A release within the site boundary or process building with significant damage	3×10^{-4}
Extensive (Es)	SEVERE – A release outside the boundary with major damage, which can be cleaned up readily, with no significant lasting consequences,	3×10^{-5}
Catastrophic (Cs)	MAJOR TO CATASTROPHIC – Widespread long term – Release from outside the fence with major damage and lasting consequences	3×10^{-6}

ProSalus Limited

Slide 7 - 37

Commercial Risk Tolerance Criteria

Defined Severity Level	Commercial Consequence Descriptors (total of: Asset loss, Product Loss, Production downtime loss & Rebuild Cost)	CBA Based on Incident Frequency/year
Minor (Ms)	£5 to < £50K	3×10^{-1}
Serious (Ss)	£50 to < £500K	3×10^{-2}
Extensive (Es)	£500K to < £5M	3×10^{-3}
Catastrophic (Cs)	£5M to < £50M	3×10^{-4}

ProSalus Limited

Slide 7 - 38

Impact Event Description & Initiating Cause

- The HAZOP is reviewed to identify all cause / consequence pairs which have a SIF included in the safeguards for the hazard scenario
- The Impact event description is the HAZOP Consequence for the hazard scenario under review
- Initiating Cause description is the HAZOP Cause for the hazard scenario under review
- These two descriptions are entered into the LOPA record sheet

Step 2 – Example Initiating events - (e.g. cause from HAZOP)

Initiating Cause	Initiating Likelihood per/yr	Initiating Likelihood Comment
Piping failure (Full breach) per 100m length	See comment	1×10^{-5} /year per 100m length
Pressure vessel residual failure	1.0E-06	Based on vessel failure
Atmospheric Tank failure	1.0E-03	Based on vessel failure
Failure of control system	0.1	Based on control system failure
Control valve	0.02	Failure to regulate
ESD valve	0.04	Spurious operation of ESD ball valve
Safety valve opens spuriously	0.01	Spurious operation of safety valve
Pump trips	0.04	Based on pump spurious stop
Operator Error (routine task with written procedure)	See comment	0.1 per opportunity
Operator Error infrequent task with written procedure)	See comment	0.01 per opportunity
Major internal leakage/tube failure within a shell and tube heat exchanger	0.01	Selected frequency assumes that exchanger is inspected annually



Functional Safety Engineering

Use Conditional Modifiers

- Use of conditional modifiers can be contentious they must be specific to the site under assessment and require to be determined by analysis. Typical conditional modifiers are:
 - Probability of ignition
 - Probability of exposure
 - Probability of Injury

ProSalus Limited

Slide 7 - 41



Functional Safety Engineering

Step 4 Identification of IPLs

- Identify BPCS protective function, If any
- List any Alarms and the operator response (written procedure required)
- Record qualifying pressure relief devices
- Document Other Safety Related Systems
 - Management Practices
 - Human Actions
 - Machine Protection Systems

ProSalus Limited

Slide 7 - 42

General Rule of Independence

To be Independent, a layer of protection shall prevent an unsafe scenario from progressing regardless of the initiating event or the performance of another layer of protection.

Given events A and B, A is independent of B if, and only if, the probability of A is unchanged by the occurrence of B.

Two events (A and B) are independent if the probability that they both occur is the product of their separate probabilities: $P(A \text{ and } B) = P(A) * P(B)$.

Independent Protection Layers Credit Factor Table					
Independent Protection Layer	PFDs	Notes			
Pressure Relief Device	1.E-02				
SIS - SIL 1	1.E-01				
SIS - SIL 2	1.E-02	Credits are zero (0) if unrestricted change allowed			
SIS - SIL 3	1.E-03				
BPCS, when independent of initiating event	1.E-01	Credits are zero (0) if unrestricted change allowed			
Internal mechanical safety trips that are independent of the SIS or BPCS	1E-1 to 1E-2	Value chosen depends on verification by vendor and testing frequency.			
Operator response under high stress, average training	5.E-01				
Operator response to Alarms and procedures, low stress, recognized event	1.E-01				
Operator response to Alarms and procedures, low stress, recognized event with more than 24 hours to resolve problem	1.E-02				
Enclosure with an elevated stack.	1.E-01				
Enclosure with attached mitigation device such as a scrubber or THROX.	1.E-02				
Containment Building capable of withstanding any credible release.	1.E-03				
Restricted Access where consequence is limited to the restricted area.	1.E-01				
Dikes when capable of mitigating the initiating event. This is an IPL only for environmental events.	1.E-02				
Other safety related protection systems	1.E-01 to 1.E-03				

Basic Rules for BPCS and Alarms

If a BPCS (whole loop) is an IE, no credit is taken for the BPCS or Alarm IPL unless they are independent systems.
If BPCS and Alarm IPLs use the same sensor, you can take credit for one IPL only.
The Alarm IPL requires a formally recorded and auditable operator action to prevent the scenario.
If a sensor failure is the IE, BPCS and Alarm IPL are not valid credits if they require the failed sensor to function.
If a final element failure is the IE, BPCS and Operator action on Alarm IPL are not valid credits if they require the failed final element to function.
If a BPCS logic solver is an IE, no credit is taken for the BPCS or Alarm IPL, unless they are independent systems
If an Alarm is an IPL, the operator must have time to prevent the scenario. No credit shall be taken if the operator has less than 10 minutes to respond. May be able to take credit if this is a recognized case in the Emergency Response plan.
Maximum of only one (1) BPCS and one (1) Alarm IPL credit are allowed for a case.
Sharing of BPCS and SIS elements may be allowed when there is evidence of adequate independence. (see rules for sharing SIS elements by the BPCS)

Step 5 - Mitigation

- Relief devices
- Flares
- Containment
- Other Safety Related Protection Systems

Then go on to consider Safety Instrumented Systems
if you still have protection gaps



Functional Safety Engineering

Rules for Pressure Relief Devices

- 1 The Pressure Relief Device either protects or it doesn't. Partial credit is not allowed.
- 2 If the Pressure Relief Device discharges to the atmosphere creating a 2nd hazard (to people, the environment or equipment), no credit is allowed. If the release to the atmosphere has an acceptable risk, credit may be taken
- 3 If the Pressure Relief Device discharges to a flare, tank, or scrubber, credit is taken
- 4 This is not a tool for deciding "No Overpressure Protection Device Needed".

ProSalus Limited

Slide 7 - 47



Functional Safety Engineering

Step 6 address SIS Requirements

List Safety Instrumented Functions if required.

The SIL of the SIF is the numerical value needed to "Close the Gap".

ProSalus Limited

Slide 7 - 48



Functional Safety Engineering

Basic Rules for SIS

- 1 SIS entries are considered last and then only if necessary to close the protection gap
- 2 A non-zero, positive value in the Protection Gap column indicates a SIS is needed.
- 3 The required SIL of the SIS is the value which closes the Protection Gap
- 4 A SIL value greater than 3 should not be allowed. Additional non-SIS IPL's are required. - or there is something wrong with the process
- 5 A zero or negative value in the Protection Gap column indicates a SIS is not needed.
- 6 A SIS with a SIL of 2 or 3 can be replaced with a combination of lower SIL provided they are independent from each other.

$$\text{SIL } 1 + \text{SIL } 1 = \text{SIL } 2 ; \text{ SIL } 1 + \text{SIL } 2 = \text{SIL } 3$$

- 7 Two (2) SIS IPL's used in the same case require separate sensors, logic solver and final element. Independent paths through the same SIS logic solver must be used.

ProSalus Limited

Slide 7 - 49



Functional Safety Engineering

Step 7

- Completely document scenario, Initiating event, IPLs. Justify and address Uncertainties and Sensitivities.
- Document the SIS requirements AND the requirements for the other Mitigation Systems

ProSalus Limited

Slide 7 - 50



Functional Safety Engineering

Example

Determination of SIL by LOPA

ProSalus Limited

Slide 7 - 51



Functional Safety Engineering

Example - Determination of SIL by LOPA

This practical exercise requires participants to determine the required SIL of a proposed safety-instrumented system using the basic principles and LOPA parameters described in this module

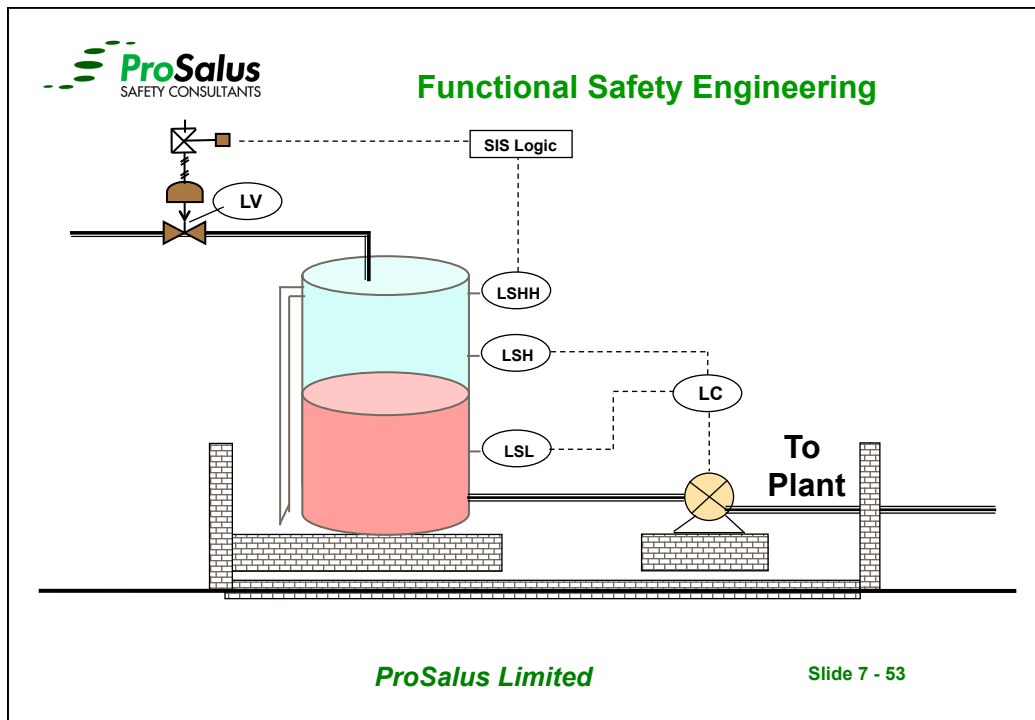
A Tank Overfill hazard has identified by the HAZOP team, two causes have been identified:

- Pump failure: 2.0 per year
- Level Control Failure: 0.1 per year

Determine the required target SIL for personnel safety of the High Level Shut Off to the tank if the tolerable risk for the hazard is $1.0E-05$

ProSalus Limited

Slide 7 - 52



ProSalus
SAFETY CONSULTANTS

Functional Safety Engineering

LOPA Worksheet for Pump Scenario

	1	Impact Event	Overpressure of Tank	
Likelihood are event/year and protection are PFD Average	2	Severity Level	S	
	3	Initiating Cause	Pump failure	
	4	Initiation Likelihood	2.0	
Protection & Mitigation Layers	5	General Design	0.1	
		Control System	0.1	
		Independent Alarm	1	
	6	Additional Mitigation, bund	0.1	
	7	Additional Mitigation,	1	
	8	Intermediate Event Likelihood	2.0E-03	
	9	Total Mitigated Event Frequency		
	10	PFDavg required		
	11	Tolerable Mitigated Event Likelihood	1.0E-05	
	11	Notes		

ProSalus Limited Slide 7 - 54

LOPA Worksheet for Level Control Scenario

	1	Impact Event	Overpressure of Tank	
Likelihood are event/year and protection are PFD Average	2	Severity Level	S	S
	3	Initiating Cause	Pump failure	LC failure
	4	Initiation Likelihood	2.0	0.1
Protection & Mitigation Layers	5	General Design	0.1	0.1
		Control System	0.1	1
		Independent Alarm	1	1
	6	Additional Mitigation, bund	0.1	0.1
	7	Additional Mitigation,	1	1
	8	Intermediate Event Likelihood	2.0E-03	1.0E-03
	9	Total Mitigated Event Frequency	3.0E-03	
	10	PFDavg required	$1.0E-05/3.0E-03 = 3.3E-03$ (SIL2)	
	11	Tolerable Mitigated Event Likelihood	1.0E-05	
	11	Notes		

Practical Exercise No: 4

Determination of SIL by LOPA



Functional Safety Engineering

Exercise No: 4 - Determination of SIL by LOPA

This practical exercise requires participants to determine the required SIL of a proposed SIS using the basic principles and LOPA parameters described in this module

Liquid is transferred manually to a holding tank before delivery to the plant, the operator must stop the pump at 75% Tank Level.

A Tank Over pressurisation hazard has been identified by the HAZOP team, two causes have been identified:

- Operator fails to stop pump : 0.1 per year
- Level Control Failure: 0.1 per year

Determine the required target SIL for personnel safety of the High Pressure Vent SIF to Flare

ProSalus Limited

Slide 7 - 57



Functional Safety Engineering

Exercise No: 4 - Determination of SIL by LOPA

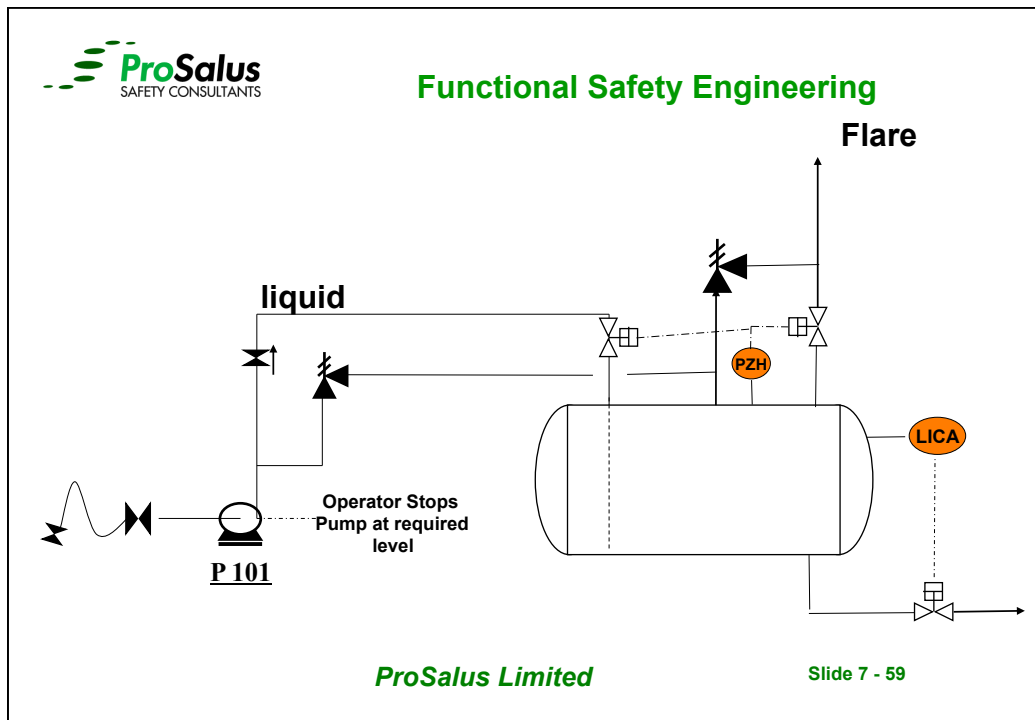
The tolerable risk for the hazard is 1.0E-05

The Holding tank has a relief valve installed which is sized for full flow and vented to Flare

The process design is not considered to be fit for purpose

ProSalus Limited

Slide 7 - 58



ProSalus
SAFETY CONSULTANTS

Functional Safety Engineering LOPA Worksheet

	1	Impact Event		
Likelihood are event/year and protection are PFD Average	2	Severity Level		
	3	Initiating Cause		
	4	Initiation Likelihood		
Protection & Mitigation Layers	5	General Design		
		Control System		
		Independent Alarm		
	6	Additional Mitigation, restricted access		
	7	Additional Mitigation		
	8	Intermediate Event Likelihood		
	9	PFDavg required		
	10	Tolerable Mitigated Event Likelihood		
	11	Notes		

ProSalus Limited Slide 7 - 60



Functional Safety Engineering

SIL Determination For Fire and Gas Systems ISA-TR84.00.07

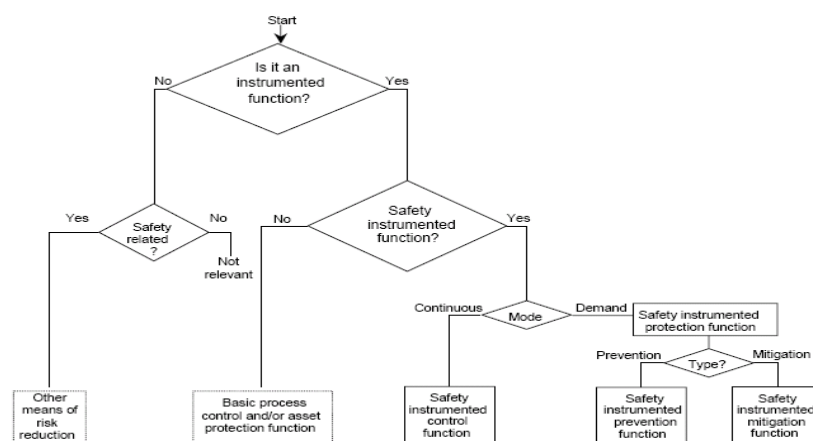
ProSalus Limited

Slide 7 - 61



Functional Safety Engineering

Relationship Between Protection Functions



ProSalus Limited

Slide 7 - 62



Functional Safety Engineering

SIPF verses SIMF

- FGS detect loss of containment by directly measuring the presence of the **released** material (gas concentration) or effects of their release (thermal radiation) to initiate mitigative actions such as:
 - Plant evacuation alarm
 - Deluge systems
 - Fire water or spray systems
 - Water curtains
- Instrument functions detect changes in process conditions without a LOC and take preventative actions to eliminate the consequence from occurring
- IEC 61511 is based on the concept that the SIF eliminates the consequence and this is why the use of performance based design methodologies for SIMF are not currently the norm in the process industries

ProSalus Limited

Slide 7 - 63



Functional Safety Engineering

Assessing Fire and Gas Systems (FGS)

- FGS design can be implemented using a
 - Prescriptive approach using national consensus standards, codes, and / or industry guidelines. (NFPA 72)
 - Risk-based approach, including the concept of designing to a targeted performance level, with an associated integrity and an acceptably-low probability of failure on demand
- However, it is difficult to apply the IEC 61511 lifecycle approach in practice due to the following three factors.

ProSalus Limited

Slide 7 - 64



Functional Safety Engineering

Factors affecting FGS Assessment

- Factor 1 - IEC 61511 techniques are suited for specific hazards that can be adequately defined using HAZOP and LOPA as an input to the risk assessment process. FGS reduce the risk of general hazards (e.g., leaks from a variety of equipment), and these hazards are difficult to define and analyze with precision without using more-advanced risk analysis techniques, such as gas dispersion modeling or fire modeling
- Factor 2 - FGS do not prevent a hazardous condition, but – rather – they mitigate the effects of the hazard. The FGS system typically reduces the magnitude and severity of a hazard instead of completely eliminating it which is a requirement of IEC61511

ProSalus Limited

Slide 7 - 65



Functional Safety Engineering

Factors affecting FGS Assessment

Factor 3 - In addition to failure of components that could render the system unavailable, a significant cause of FGS ineffectiveness is due to inadequate positioning of FGS sensors to detect the hazardous condition. Even if very high SIL targets can be achieved in FGS design and testing (in terms of low average probability of failure on demand of the instrumented function), sufficient reduction in risk will not occur unless detector placement and coverage is very high.

Therefore, the detector placement and coverage problem requires study with the same quantitative rigor as average probability of failure on demand.

ProSalus Limited

Slide 7 - 66



Functional Safety Engineering

Factors affecting FGS Assessment - Final Elements

Another significant cause of FGS ineffectiveness is due to the incapability of the mitigation final elements (e.g. fire water system, foam deluge, water curtain, ventilation system) to perform their function with a high probability of success.

Effectiveness of the mitigation function is dependent on:

- stopping the process and removing the hazardous material
- applying fire water with the appropriate flow and spray characteristics
- Initiating alarms to enable personnel to get to safety

ProSalus Limited

Slide 7 - 67



Functional Safety Engineering

ISA-dTR84.00.07 Performance-based FGS Analysis Procedure

1	Screen to determine if FGS function is required and define control volumes
2	Identify Risk Scenarios
3	Analyze Consequences
4	Analyze Hazard Frequency
5	Unmitigated Risk Assessment
6	Identify Requirements for FGS Risk Reduction
7	Initial FGS System Design
8	Assess Detector Coverage
9	Assess FGS Safety Availability
10	Mitigated Risk Assessment
11	Modify FGS System Design

ProSalus Limited

Slide 7 - 68



Functional Safety Engineering

Conclusions on FGS Assessment

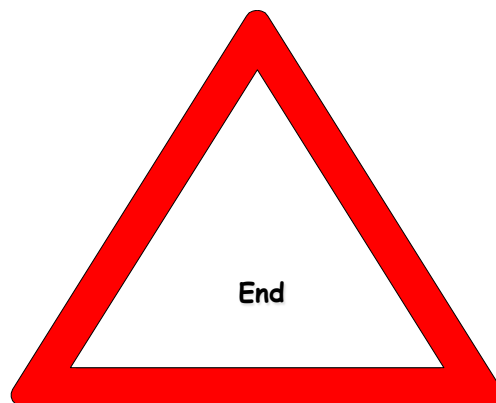
- FGS assessment requires advanced techniques for analysis not normally considered part of the C&I Function more related to Process Safety / Technical Safety Function and covered by the QRA
- Significant cause of FGS ineffectiveness is inadequate positioning of detectors and final elements and only calculating the PFD of the system components is not rigorous enough
- RRF only achieved if detector placement & coverage is high
- RRF is also dependent of capability of Final Element (Fire water etc)
- SIL is insufficient to properly define the design basis for FGS SIF
- Design basis based on performance criteria –
 - Percentage Detector Coverage
 - Percentage Mitigation Effectiveness
- Remember relevant standards must be applied (e. g. EN 54 / NFPA 72)

ProSalus Limited

Slide 7 - 69



Functional Safety Engineering



ProSalus Limited

Slide 7 - 70